CHAPTER 1. Scope

1.1 Identification

This document describes software requirements for the Defense Information Infrastructure (DII) Common Operating Environment (COE) platform services: Management and System Administration Services, Security Services (including Security Administration Services), Communications and Network Services, Distributed Computing Services, Data Management (Data Access) Services, and Presentation Services (composed of the Executive Manager functional area and the Multimedia functional area).

1.2 System Overview

The COE is intended for use by all Department of Defense Command and Control Systems as the infrastructure on which they reside. The COE consists of an integrated architecture made up of hardware and software which provides standard, modular, system support and application support software for a tailorable set of functional application software.

This document specifies the software requirements for the DII COE.

Service and agency unique requirements are outside the scope of this document.

1.2.1 Management Services

Management Services is defined as the ability to manage all hardware and software resources in a heterogeneous, distributed information system. Efficient and effective management of DII is extremely important to the functional user community supporting the defense of the United States. Maintaining operations of a vast and diverse array of information resources interconnected with Local Area Networks (LAN) and Wide Area Networks (WAN) is a major undertaking; however with strict guidelines and robust tools the task will be better handled. The purpose is to ensure that the information systems continue to operate in support of the efforts of the warfighters and supporting organizations during peace-time, crisis and war-time operations. This document addresses and defines the functions and requirements of the Management Services within the DII COE.

Management Services includes the following areas, which are often implemented separately due to the lack of integrated tools:

1. Network Administration: Network Administration is defined as those services that support the configuration of network elements, establishment of network connectivity, and ensuring continuous network operations.
2. System Administration: System Administration is defined as the services that are required to ensure effective and efficient operation of those elements of the information system that are not an integral part of the network and to manage the configuration and operations of workstations, servers, applications and the user environment on a day-to-day basis.
3. Security Administration: Security Administration is defined as the services required to manage, configure, operate and maintain information system security functions and to ensure that the system continues to meet security requirements as defined by the accrediting authority.

This document includes the functional requirements for management services to support these three areas. Because these areas are interdependent, the requirements are addressed in terms of management services as an integrated set of functions. These functions include the five System Management Functional Areas (SMFAs) defined by the International Organization for Standardization (ISO): configuration management, fault management, performance management, security management, and accounting management. However, since accounting management entails functions necessary for charging fees to users for the use of system resources, and it is not the intention of the government to need those capabilities, accounting management will not be addressed further in this document.

Management Services are provided in accordance with Management Domains as defined by the ISO. A management domain is a bounded set of information system resources that are under the management and control of a single set of management tools. Three levels of management have been defined for DII: (global, campus, and site). There is a single manager for the global level, while the campus and local levels will be implemented numerous times depending on Command and site configurations. Each implementation constitutes a management domain.

1.2.1.1 Network Management

DII will be our nation's conventional, joint command and control (C2) system. DII must be an instantaneously flexible system that collects, transports, processes, disseminates, and protects C2 information. DII will support warfighting actions that are essential to the National Command Authorities (NCA) and subordinate elements in the generation and decisive application of national power. DII will operate over a global network employing communications, computers, surveillance, reconnaissance, intelligence, and space based systems in order to perform the C2 mission. DII will include both fixed and mobile platforms that will support forces for joint and combined operations throughout the spectrum of conflict anytime and anywhere in the world with compatible, interoperable, and integrated Command, Control, Communications, Computers, and Intelligence (C4I) systems. DII also will allow response to natural emergencies and/or man-made disasters when military support is appropriate and directed to respond.

Development began on DII in the 1st quarter of FY-94. DII will use state-of-the-art technology (Sun data servers and other Commercial Off-the-Shelf (COTS) hardware and software products). The DII architecture at its simplest is a suite of servers made up of at least one ORACLE database server and two application servers. The ORACLE database server, usually a Sun SPARCserver 1000 or Sun SPARCcenter 2000, serves as the repository for all ORACLE databases. At most sites, all user accounts and user data also will be stored on the ORACLE database server, as will other data typically stored on file servers. Certain applications will reside on the ORACLE database server, but the majority of the applications will reside on the application servers which are SUN workstations. The application servers also will contain certain COTS and Government Off-the-Shelf (GOTS) services that will be used by all DII platforms. DII will have Initial Operational Capability (IOC) at 37 locations (see Table 1. An additional 18 locations are planned at this time (see Table 2.

Table 1. DII Initial Operating Capability (IOC) Locations

Acronym	Command and Location
ACC	Air Combat Command, Langley AFB, Hampton, VA
ACOM	Atlantic Command, Norfolk, VA
AFMC	Air Force Material Command, Wright-Paterson AFB, OH
AMC	Air Mobility Command, Scott AFB, IL
ANMCC	Alternate National Military Command Center, Ft Ritchie, MD
ARCENT	Army Central Command, Ft McPherson, GA
AREUR	Army European Command, Heidelburg, Germany
ARPAC	Army Pacific Command, Ft Shafter, HI
CENTAF	Central Command, Air Force, Shaw AFB, SC
CENTCOM	Central Command, MacDill AFB, Tampa, FL
CINCLANTFLT	Commander-in-Chief Atlantic Fleet, Norfolk, VA
CNO	Chief of Naval Operations, Pentagon, Washington DC
EUCOM	European Command, Stuttgart, Germany

FORSCOM	Force Command, Ft McPherson, GA
HQAF	Headquarters of the Air Force, Pentagon, Washington DC
HQDA	Headquarters, Department of the Army, Pentagon, Washington DC
HQMC	Headquarters, Marine Corp, Navy Annex, Arlington, VA
JTO	Joint Training Organization, Scott AFB, IL
MARFORLANT	Marine Forces Atlantic, Camp Lejeune, NC
MARFORPAC	Marine Forces Pacific, Camp Smith, HI
MSC	Military Sealift Command, Navy Yard, Washington DC
MTMC	Material and Movement Command, Army, Washington DC
NAVCENT	Navy Central Command (Rear), MacDill AFB, Tampa, FL
NAVEUR	Navy European Command, London, United Kingdom
NMCC	National Military Command Center, Pentagon, Washington DC
PACAF	Pacific Air Force, Hickam AFB, HI
PACFLT	Pacific Fleet, Makalapa, HI
PACOM	Pacific Command, Camp Smith, HI
SOCOM	Special Operations Command, MacDill AFB, Tampa, FL
SOUTHCOM	Southern Command, Quarry Heights, Panama
SPACECOM	Space Command, Peterson AFB, CO
STRATCOM	Strategic Command, Offutt AFB, NE
TRANSCOM	Transportation Command, Scott AFB, IL
USAFE	United States Air Force, Europe, Ramstein AB, Germany
USASOC	United States Army Special Operations Command, Ft Bragg, NC
USFK	United States Forces, Korea, Yongsan Garrison, Republic of Korea
USFK2	United States Forces, Korea 2, Taegu, Republic of Korea

Table 2. DII Post IOC Locations

Acronym	Command and Location
AFSPACECOM	
AFSOC	
ALCOM	
ARSPACECOM	
COMICEDEFOR	
COMUSFORAZ	
FC-DNA	
HQ-DNA	Headquarters, Defense Nuclear Agency
JSOC	
NAVCENT	
NAVSOUTH	
NAVSPACECOM	
NAVSPECWARCOM	
SOCCENT	
SOCSOUTH	
SOUTHAF	
USARSO	
USFJ	

DII will replace the World-Wide Military Command and Control System (WWMCCS) Intercomputer Network (WIN), which is a centrally managed information processing and exchange network consisting of large-scale computer systems at geographically separate locations, interconnected by a dedicated wide-band, packet-switched communications subsystem. The architecture of the WIN consists of WWMCCS-standard AN/FYQ-65(V) host computers and their WIN-dedicated Honeywell 6661 Datanets and Datanet 8's connected through Bolt Beranek and Newman, Inc. (BBN) C/30 and C/30E packet switching computers called Packet Switching Nodes (PSNs) and wideband, encrypted, dedicated, data communications circuits. DII software applications largely will consist of existing WWMCCS software and other software modified and integrated for DII use via a "Best of Breed" selection process.

Network Management (NM) will support DII and it's interconnected hardware and software by providing a platform for the management of distributed work group networks. NM will manage devices from different manufacturers. It will involve all the elements of the network: network hardware, network protocols, hosts, operating systems, and application software. It will be able to adjust to physical changes in the network as well as changes in mission and policy.

DII will use the Secret Internet Protocol Router Network (SIPRNET), which is part of the Defense Information System Network (DISN), for its Wide Area Network (WAN) data transport. DII will operate at the SECRET System High mode. However, three nodes of WWMCCS Honeywell equipment will be kept operational to support the remaining top secret mission requirement of the DII (referred to as TS3). TS3 also will use the SIPRNET for data transport through end-to-end encryption devices.

The DISN uses a three layer model to define the different areas of NM responsibility. The top management center is referred to as the Global Control Center (GCC) which is operated by the DISA C4I Network Systems Management Division (D31). The GCC provides management oversight for the deployed networks of the Defense Information Infrastructure (DII) for which DISA has NM responsibility. The second layer is comprised of the Regional Control Centers (RCCs). The RCCs are responsible for the day to day operations of the networks under their immediate control. They are geographically oriented with several centers dispersed across the United States, a center located at the DISA European facilities to cover Europe, and another located at the DISA Pacific facilities to cover the Pacific assets. The RCCs are responsible for the DISA assets within their areas and operate as peers to each other. The RCCs and the GCC are responsible for DISA assets only. The third layer of the hierarchy model is the Local Control Centers (LCCs) which belong to the individual subscriber communities. These management centers control or monitor the assets owned by the individual Service/Agencies connected to the WANs. The DII premise routers are included in this list of equipment. In the case of the DII, the community must establish an LCC to manage the DII assets.

The major concern of system and NM responsibilities is determining where the demarkation point exists between DII communications equipment and the DISN's SIPRNET. This has been discussed in terms of physical locations, management control, and the ownership of the communications equipment. As stated above, the DISA GCC and RCCs do not manage assets belonging to subscriber communities (in this case, DII). While this definition provides a starting point, it does not provide the exact physical location of change over. The demarkation point has been defined more completely by stating the RED side of the cryptographic equipment in the subscriber's location is where DISA responsibilities end and the subscriber's responsibility begins for serial access circuits. In the case of ethernet connections, the subscriber is responsible from the ethernet port connector to their assets. Approximately 95% of DII to SIPRNET access connections will be serial in nature with the other 5% being ethernet.

The SIPRNET is the new, worldwide router-based network replacing the older X.25-based packet switched network (the Defense Secure Network One (DSNET1) of the Defense Data Network (DDN)). The initial SIPRNET backbone router network went online 3 March 1994. Subscribers started coming on line shortly thereafter. The SIPRNET WAN (as of 31 May 1995) consisted of a collection of 31 backbone routers interconnected by high-speed serial links to serve the long-haul data transport needs of secret-level DoD subscribers. Additional SIPRNET backbone routers are being planned to meet increased customer requirements. SIPRNET supports the DoD standard Transmission Control Protocol/Internet Protocol (TCP/IP) protocol service. Subscribers within the DoD and other Government Agencies are able to use the SIPRNET for passing datagrams at the Secret-Not Releasable to Foreign Nationals (SECRET-NOFORN) classification level.

The DII community relies heavily on the SIPRNET for its WAN infrastructure. As such it is imperative that a strong working relationship exist between the SIPRNET RCCs and the DII Management Center (DMC) for the DII community. It is also important to note that unlike the WWMCCS environment and DSNET2, the DII does not enjoy exclusive use of the SIPRNET. The DII community only makes up about 15% of the subscribers on the SIPRNET.

The DMC is composed of three major locations with supporting offices. The three sites are the DMC-Pentagon located in the Pentagon operating off of the National Military Command Center (NMCC), DMC-Site R operating off of the Alternate NMCC (ANMCC) located at Site R, and the DMC-OSF operating at the DISA Operational Support Facility (OSF) located in Sterling, Virginia. The DMC will provide 24 hours a day, 7 days a week, operational support for managing the DII.

The SIPRNET is managed by the DII/DISN RCCs which provide day-to-day operational management. The RCCs use Sun Net Manager, HP Openview, and CiscoWorks to evaluate any router on the SIPRNET. Data is collected on various traffic patterns within the SIPRNET. Data collection includes total router traffic sent and received. The amount of Internet Protocol (IP) traffic from outside the WAN structure is referred to as the exterior load. Finally, system delays (elapsed times) are measured between all routers and ports using the PING tool. Measurements are in packets per second terms. The results of the various data collecting efforts are kept on file for long term management of the router-to-router traffic.

The tactical subscriber connections will be serial connections provided by satellite communications equipment via the Defense Satellite Communications System (DSCS) through a Defense Communications System Entry Point (DCS-EP). These EPs provide worldwide access for deployed Joint Task Forces (JTFs). The ITSDN gateway routers support the standard TCP/IP protocol suite for serial connections to the gateway routers.

Deployed DII forces may rely on the ITSDN capabilities to reach the SIPRNET WAN. The DII/DISN RCCs provide day-to-day operational management of the ITSDN routers. Again, it is imperative that a strong working relationship exist between the RCCs and the DMC so the status of WAN assets supporting the deployed DII forces can be available readily.

Communications servers (CSs) are being added to the SIPRNET during the 4th quarter of FY-95 for the general DoD secret community. These CSs will be managed by the DII/DISN RCCs responsible for managing the SIPRNET. The CSs will give remote subscribers the capability to access the SIPRNET WAN via dial-in. This capability will be especially valuable for those subscribers who do not have the need for a dedicated connection, for those subscribers who are continually travelling on Temporary Duty (TDY), or for deployed tactical subscribers who have access to a telephone system.

Both strategic and tactical DII forces will be able to take advantage of the DISN CSs available on the SIPRNET WAN provided they are registered users. Again, the day-to-day operational management of the SIPRNET CSs will be by the DII/DISN RCCs. A strong working relationship between the RCCs and the DMC is required. If DII users register for this dial-in service the DISN RCCs will be asked to provide the status of SIPRNET CS assets to the DMC.

1.2.1.2 System Administration

The purpose of the system administration area is to provide requirements for the system administration software components of individual applications to be used within the DII COE. Each service may choose how to implement the system administration for its applications so long as it conforms to the requirements and DII standard formats and protocols. The goal is to establish applications that can communicate through standard Application Programming Interfaces (APIs). The system administration requirements contained within this document shall be used throughout the other DII functional areas to perform similar functions.

System administration provides the means whereby a person can manipulate the controllable aspects of the software portions of the system to meet user needs. It is a collection of diverse mechanisms for altering the DII infrastructure configuration. It is intended to provide an effective way for moderately skilled personnel to keep the DII application common infrastructure reliable and configured to the needs of each site and each user.

The system administrator is the person who both carries out user requests and acts as the intelligence in the control loop on the system to ensure continued system stability. To help put a consistent set of buttons at the disposal of the system administrator, commonality between applications is needed. Just as DII's segment approach has greatly eased the difficult task of loading and configuring a wide range of applications on a UNIX platform, the system administration aspects of each segment needs to be regularized and packaged uniformly.

The "System" in System Administration refers to one DII site. A typical site has two application servers and one database server plus a number of PC's/TAC-4/... xterm'ed into the applications servers. Some sites only have application servers and are remotely using another site's database server. While the system administration software shall be installed on all application and database servers, it is the ultimate goal to have a system administrator be able to perform his duties regarding any of the servers from any other server.

System Administration has been the "neglected" part of DII. It is a murky domain of UNIX details, bug workarounds, and heavy on-the-job training. Yet System Administration is a big usability determiner — if your car's broke you can't go anywhere. If it breaks down a lot, you'll never trust it. As DII replaces WWMCCS operationally, the ability to keep it working in the face of shifting needs, software, hardware, and the unanticipated impacts of various failures is a must-have. Based upon the down-hill principle, a vast quantity of changing system administration minutiae is required knowledge of the system administrator. Mastery of the entire body of information for all applications probably exceeds the ability of any one human being. The DII COE's System Administration functional area is dedicated to making this a do-able task.

1.2.2 Security Services

This document contains the software security requirements for the DII COE, but does not address the overall security requirements of systems built using the DII. The overall security requirements will be met by the COE security services software and other security disciplines (e.g., administrative, physical, personnel). Security Services are one of six platform services defined in the *Architectural Design Document for the Defense Information Infrastructure Common Operating Environment* (DISA, 1996), which is intended to be compliant with the *Technical Architecture Framework for Information Management* (DISA, 1995), including Volume 6, the Department of Defense Goal Security Architecture (DISA, 1994). The security requirements specified in this document will be allocated across the COE platform services areas.

The Security Services will provide security services across a heterogeneous environment. These security services are broken down into five areas: Accountability, Access Control, Confidentiality, Integrity, Non-repudiation, and Availability.

The DII will initially support a System High mode of operation. The objective of the DII is to support a Multi-level Secure (MLS) mode of operation, which will demand additional security requirements above those required for System High operation. Looking to the future, however, this SRS does include some MLS mode requirements.

Service, agency and system unique security requirements are outside the scope of this document.

1.2.3 Communications Services

This document also describes the Communications Services of the DII COE. Dependencies and interactions between the Communications area and other functional areas are discussed to help clarify where Communications Services begin and end and how these services fit into the overall scheme of things.

1.2.3.1 Communications Services Overview

Communication Services is defined to be an infrastructure of coordinated services primarily supporting connectivity and data exchange between one GCCS system or workstation and another GCCS system or workstation. Communications services provide the capability to send, receive, forward, and manage electronic and voice messages. They also provide real-time information exchange services in support of interpersonal conferences. These services include:

1. Personal Message Transfer services, including the capability to send, receive, forward, store, display, and manage personal messages.
2. Organizational Message Transfer services, including the capability to send, receive, forward, display, retrieve, prioritize, and manage formatted and freeform organizational messages. Organizational messages should use standard data interchange formats and may include any combination of data, text, audio, graphics, and images. This includes the capability to review and authenticate messages. Incoming message processing services include receipt, validation, distribution, and dissemination of incoming unformatted messages based on message profiling, message precedence, and system security restrictions. User support services include the selection and display of messages from a message queue, on-line management of search profiles, search and retrieval of stored messages based on message content comparison to queries formulated by the analysts, and composition of record messages for transmission. Outgoing message processing services include coordination by Command’s staff organizations, authorized release, and verification of record messages prior to transmission.
3. Enhanced telephony services, including call forwarding, call waiting, programmed directories, teleconferencing, automatic call distribution (useful for busy customer service areas), and call detail recording. Enhanced telephony service also includes precedence and preemption capabilities.
4. Shared screen services that provide audio teleconferencing with common workstation windows between two or more users. This includes the capability to refresh windows whenever someone displays new material or changes an existing display. Every user has the capability to graphically annotate or modify the shared conference window.
5. Teleconferencing services that provide two-way video or multi-port transmission between different sites. These services include:
    - full motion display of events
    - participants in a bi-directional manner
    - support for the management of directing the cameras including:
        - ranging from fixed position
        - sender directed
        - receiver directed
        - automated sound pickup.
6. Broadcast services that provide one-way audio or audio/video communications services between a sending location and multiple receiving locations. Broadcast services also includes data communications services.
    - Combat Net Radio services that provide audio communications between multiple sending and receiving locations.
    - Conferencing services that allow groups to participate in conferences. These conferences may not occur in real time. Conferees or invited guests can drop in or

out of conferences or subconferences at will. The ability to trace the exchanges is provided. Services include exchange of documents, conference management, recording facilities, and search and retrieval capabilities.

Communications Services, as defined in the DoD Technical Architecture Framework for Information Management (TAFIM), are broken into the following areas:

1. Message Transfer Services
2. Voice Communications
3. Visual Services
4. Information Transfer Services
5. Information Technical Service Management
6. Network Services

1.2.3.2 Message Transfer Services

One end of the Message Transfer service is bounded by and includes the logical system input/output devices. This does not necessarily include down-line conveyance vehicles such as cryptos, modems, radios, etc. The other end of Communication service is bounded by and includes the message collection and distribution functions supporting client applications and other service areas such as the Message Processing Services and message processing engines. Using this definition of the Message Transfer service and its boundaries allows for a segregatable and certifiable (where appropriate) communications subsystem that can be utilized for GCCS with controlled mechanism for handling extensions and customizations of services.

These services allow a user to prepare, send, and receive messages. The most fundamental Message Transfer service supports text-based Message Transfer only. Increasingly more sophisticated Message Transfer services provide support for various types and formats of information in addition to text, and will include data files, graphics, facsimile, and voice. The Message Transfer services used by all DoD include two main categories:

1. The Automated Data Information Network (AUTODIN) provides the current capabilities for organizational Message Transfer services for USMTF messages.
2. The Defense Message System (DMS) will provide target capabilities for personal and organizational Message Transfer services.

However, the Message Transfer services include many other DoD service specific networks, interfaces, and protocols that provide for information transfer between sites and systems.

The term "message" refers to the logical collection of data bits bundled by applying the rules for the format of the data (character-oriented, bit-oriented, graphics, voice, data, etc.) . For example; Formatted Record messages are bounded by applying the rules of JANAP 128, ACP 126M, ACP 127, etc . Tactical Data Information Link (TADIL) binary messages are bounded by frame labels indicating the applicable series message and the fixed size of the given message. These messages are bounded by applying the rules of OS411 and OS516. A graphics for such as TIF, BMP, etc. has a specified format as do audio files.

Message Transfer services includes such areas as physical interfaces, protocols, interface control, data bounding into messages, message identification, message storage, message retrieval, message logging, message notification, message alerting, message queuing, message validation, message collection, and message distribution.

In postal service terms, the Message Transfer Service looks at the envelope of the message not the actual content. The envelope conveys information about the source, destination and priority of the message; whereas a user or client application handles the processing of the actual message content.

In terms of the International Standards Organization (ISO) Open Systems Interconnection (OSI) Reference Model (ISO 7498/ITU-T X.200), the GCCS Message Transfer services notional architecture (See Figure 1. Notional Communications Architecture) can be described in terms of the 7 layer reference model (See Figure 2. Notional Architecture and OSI Layers). In this context, client applications (layer 7) are establishing virtual connections to their counterpart applications on remote hosts via the Message Transfer services of GCCS. Data flows amongst these client applications without their direct involvement or knowledge of the underlying conveyance mechanisms. Although this model is useful for describing interfaces between open systems some difficulties are found when applying the model to older/closed system architectures that will continue to interface to GCCS. Although these older systems/interfaces are being phased out, it will still be many years before that happens. Therefore, it is unrealistic to propose a communication services solution that ignores these existing interfaces.

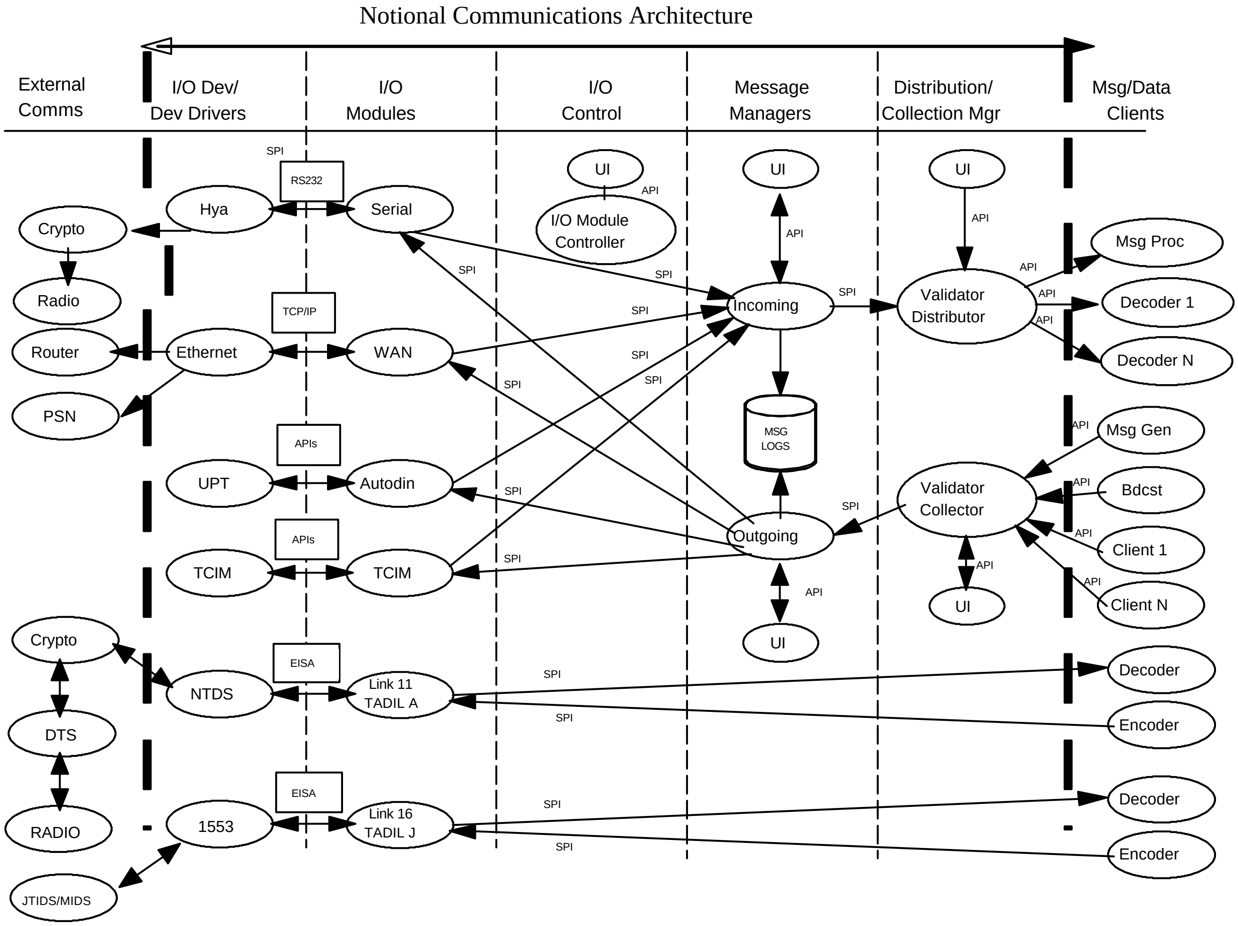


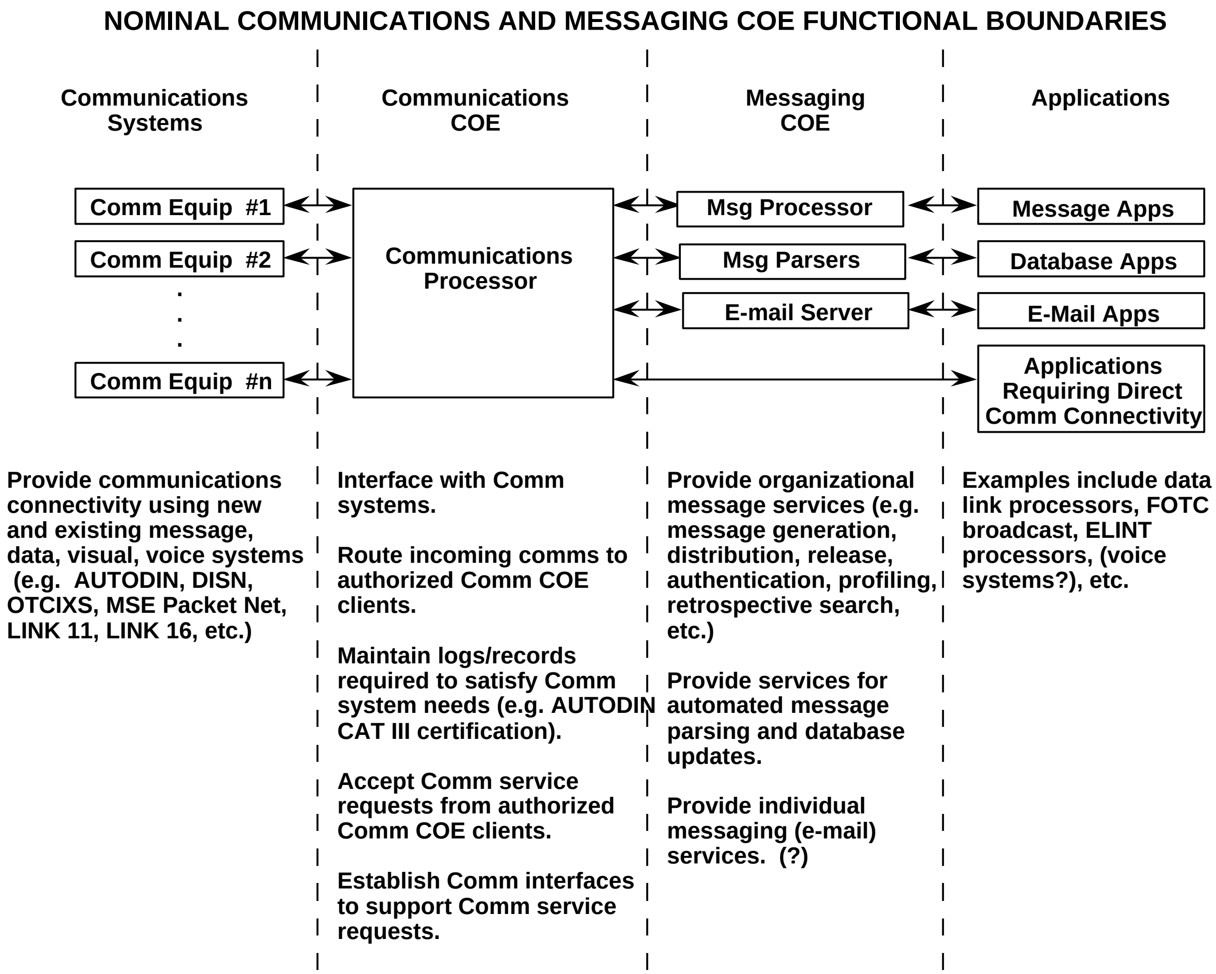
Figure 1. Notional Communications Architecture

Notional Communications Architecture

	I/O Device Device Drivers	I/O Modules	I/O Control	Message Managers	Distribution/ Collection Mgr
Application (7)				x	x
Presentation (6)				x	
Session (5)		x	x		
Transport (4)	x	x			
Network (3)	x				
Data Link (2)	x				
Physical I/F(1)	x				

Figure 2. Notional Architecture and OSI Layers

Figure 3. Nominal Communications and Messaging presents a depiction of the Nominal Communications and Messaging and indicates at a high level how the various services interact to provide for Communications services and its clients.



Provide communications connectivity using new and existing message, data, visual, voice systems (e.g. AUTODIN, DISN, OTCIXS, MSE Packet Net, LINK 11, LINK 16, etc.)

Interface with Comm systems.

Route incoming comms to authorized Comm COE clients.

Maintain logs/records required to satisfy Comm system needs (e.g. AUTODIN CAT III certification).

Accept Comm service requests from authorized Comm COE clients.

Establish Comm interfaces to support Comm service requests.

Provide organizational message services (e.g. message generation, distribution, release, authentication, profiling, retrospective search, etc.)

Provide services for automated message parsing and database updates.

Provide individual messaging (e-mail) services. (?)

Examples include data link processors, FOTC broadcast, ELINT processors, (voice systems?), etc.

Figure 3. Nominal Communications and Messaging

1.2.3.3 Voice Communications

These services provide inter-human voice communications and include real-time (e.g., plain-old-telephone-service and air-to-ground) and stored voice messages. Telephone services and radio services are specialized forms of voice communications services. An overall voice communications service may actually consist of individual telephone services and radio services. The voice communications services must employ information transfer services for actual voice transmission.

1.2.3.4 Visual Services

These services generally provide mechanisms for capturing, processing, transferring, and displaying visual information. This service area includes imagery, video, and facsimile. The services for transferring the visual information are in addition to the information transfer services. Visual services must employ information transfer services for actual information transmission.

1.2.3.5 Information Transfer (IT) Services

These services support the transfer of C^{4}I information (e.g., voice, data, video, messages, images, etc.) between users and/or C^{4}I systems.

1.2.3.6 Information Technical Service Management

Services supporting the management, integration, accounting, and security of the other IT Services and the systems, facilities, and resources comprising those services. This service includes specific services such as network management, message management, and electronic key management. These services are used by Communications Functional area but are covered by the Network Management Functional area SRS.

1.2.3.7 Network Services

Network services are provided to support distributed applications requiring data access and applications interoperability in heterogeneous or homogeneous networked environments. They include the following functional areas :

1. **Data communications**, which include protocols for reliable, transparent, end-to-end data transmission across communications networks.
2. **Personal/microcomputer support** for interoperability with systems based on a variety of operating systems.

1.2.4 Distributed Computing Services

The focus of the COE's distributed computing component is on distributed computing capabilities that permit procedures and objects to be invoked on remote hosts as though they were local to the calling module. In addition to these basic capabilities, the distributed computing component will include a variety of enabling services, such as security, time, persistence, and naming; many of these services are required for the development of applications that are distributed. The two fundamental technologies that will be implemented in the COE are the Distributed Computing Environment (DCE) and the Common Object Request Broker Architecture (CORBA), including some related services; These technology choices are based on requirements from Department of Defense (DoD) services and related agencies.

This document focuses on specifying requirements for the implementation of these basic technologies in the COE, as well as for related capability requirements that may not be addressed by those two basic technologies. Related capability requirements may include requirements relating to the integration of the distributed computing component with other components or capabilities in the COE.

NOTE: The requirements specified herein assume a familiarity with the concepts of distributed computing and with the two specific technologies, DCE and CORBA, that are being used to implement the distributed computing component of the COE.

1.2.5 Data Management (Data Access) Services

This document establishes the functional, performance, and verification requirements for the Data Access Services functional area of the DII COE. The Data Access Services functional area includes File Access, File Management, Database Access, and Database Management.

1.2.5.1 Data Management Services Functional Area Overview

Data Access Services (DAS) provide a set of consistent client-server oriented data administration and data management services for mission and support applications. These services isolate vendor-unique implementations of data access and provide applications a means of avoiding dependencies on physical access models. These services also provide data management functions for access to distributed (local and remote) database management systems.

1.2.5.1.1 Data Management Services Capabilities

Data Management functions are divided into two areas: File Access and Database Access. File Access provides the capability to develop COE infrastructure and mission applications which are file system independent and portable across UNIX (POSIX) and Windows hardware platforms. The File Access functions are a common set of capabilities (open, close, rename, and etc.) available across the target platforms, while providing hooks to access hardware unique functions as required. These services define file naming standards and validation routines to prevent the creation of filenames which contain non-portable characteristics. These services are available for distributed (local and remote) operations.

Database Access functions are a common set of capabilities (open database, select database, rename, insert, query and etc.) available across the target platforms, while providing hooks to access database and hardware unique functions as required. Database Access addresses the use of Data Manipulation Language (DML) and Data Definition Language (DDL) as well as the selection of the SQL interfaces to be supported.

1.2.5.1.2 Data Administration Capabilities

Data Administration functions are divided into two areas: File Administration and Database Administration. File Administration functions are a common set of capabilities (backup, archive, restore, and etc.) available across the target platforms, while providing hooks to access hardware unique functions as required. These services are available for distributed (local and remote) operations.

Database Administration functions are a common set of capabilities (archive database, import, export, and etc.) available across the target platforms, while providing hooks to administer databases. Database Administration addresses the use of DDL, access to data, location of the data, and the distribution of data.

1.2.6 Presentation Services

The Presentation Services functional support area defines the functionality of the services required to manage processes and the graphical user interface. It also defines the software tools required to manipulate and manage multimedia information. These services are further defined in the two categories of Executive Manager and Multimedia.

1.2.6.1 Executive Manager System Services Overview

The purpose of the executive manager functional area is to provide process management services for both batch and transaction processing, management of information flow between applications, and notification of critical events. Process management includes information processing, job and process control, menu executive services, security services, and queuing services. All information processing features should be available to Ada and C programs.

1.2.6.2 Multimedia System Services Overview

Multimedia services provide the capability to manipulate and manage information consisting of coordinated text, graphics, audio, imagery, animations and/or video. Multimedia services may be employed in a variety of application contexts, including multimedia presentations (e.g., situation assessment displays, course of action briefings, after action reviews), access to multimedia information collections (e.g., for intelligence analysis), collaboration among users (e.g., analysis, planning, course of action selection) including the use of multimedia mail and conferencing (e.g., video, audio), mission rehearsal, and training.

1.3 Document Overview

Section 2 lists documents referenced and documents that provide guidance applicable to this specification.

Section 3 details the requirements for each of the DII COE platform services: Management and System Administration Services, Security Services, (including Security Administration Services), Communications and Network Services, Distributed Computing Services, Data Management (Data Access) Services, and Presentation Services (composed of the Executive Manager functional area and the Multimedia functional area).

The Security Services include Accountability, which is comprised of identification and authentication and security audit; Availability; Confidentiality, which is comprised of discretionary access control, mandatory access control, labeling, trusted interfaces, object reuse, and data confidentiality; Integrity, which is comprised of data integrity, system integrity, and non-repudiation; and some Assurance requirements, which is comprised of system architecture and trusted facility management. Other assurance requirements are presented in Section 4.

Section 4 identifies the qualification provisions including the methods used to ensure that the requirements in Section 3 have been met.

Section 5 addresses the traceability of each requirement from an appropriate source, such as a requirements document; in the case of security, this may also be a security policy. Section 5 also includes implementation priorities for each requirement.

Section 6 contains acronyms, abbreviations, schedules, and a list of terms and definitions needed to understand this document.